Drew Findling
PHV-21739-2019
Findling Law Firm P.C.
3490 Piedmont Road, Suite 600
Atlanta, GA 30305
404-460-4500

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA Plaintiff V. DALE BEHM; and JOSHUA CLARK Defendants.	CASE NO. 3:20-CR-00321 EMC NOTICE OF MOTION TO SUPPRESS FRUITS OF SEARCH WARRANTS

MOTION TO SUPPRESS

COMES NOW Defendant Joshua Clark, by and through undersigned counsel, and moves this court to suppress communications obtained from Mr. Clark's email accounts, josh.clark@transpacificpolymers.com and josh.clark@hammertexas.com, acquired pursuant to the search warrants issued June 12, 2019 and October 25, 2019, respectively. The communications were obtained in violation of the Fourth Amendment to the United States Constitution. Mr. Clark further requests an evidentiary hearing be held on the present motion. The following memorandum is offered in support.

Respectfully submitted,

Dated: October 14, 2021

s/Drew Findling
Drew Findling
PHV-21739-2019

TABLE OF CONTENTS

TABLE OF AUTHORITIES

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

In 2019, the Government obtained two search warrants for virtually every piece of information contained in or related to two email accounts belonging to Joshua Clark. The warrants were authorized in reliance on affidavits that failed to establish probable cause for the crimes alleged and relied on stale information. The resulting search warrants were overbroad and violative of the Fourth Amendment. This litany of failures resulted in the Government seizing and reviewing tens of thousands of emails with little, if any, regard for the Defendant's right to privacy. The warrants are fundamentally insufficient to justify seizure and unfettered search of the email accounts belonging to Joshua Clark. Accordingly, Defendant respectfully requests that the Court invalidate the warrants and suppress all evidence obtained in the searches. Furthermore, Defendant respectfully requests an evidentiary hearing on the motion.

II. FACTUAL BACKGROUND

A. Overview of the Investigation

On August 12, 2020, the Grand Jury returned an indictment in the present case, charging five defendants with eight counts of criminal conduct. All of the defendants were charged in Counts One through Twenty Eight: Conspiracy to File False Claims (18 U.S.C. § 286) (Count One), False, Fictitious, or Fraudulent Claims (18 U.S.C. §§ 287 and 2) (Counts Two Through Sixteen), and Wire Fraud (18 U.S.C. §§ 1343 and 2) (Counts Seventeen Through Twenty Eight). All defendants but Dale Behm were charged in Counts Thirty-nine through Forty-Two: Laundering of Money Instruments (18 U.S.C. §§ 1956(a)(2)(A) and 2), along with forfeiture allegations. Defendants Joshua Clark, Joshua Stanka, and Michael Choy were charged in Counts Thirty-One through Thirty-Eight: Money

Laundering (18 U.S.C. §§ 1957 and 2). Yong Heng Liang, a/k/a Colin Liang, was charged individually in Counts Twenty-Nine through Thirty: Mail Fraud (18 U.S.C. §§ 1341 and 2) and Count Forty-Three: Falsification of Records to Obstruct Investigation (18 U.S.C. §§ 1519 and 2).

The Government alleges a wide-ranging scheme in which the named actors conspired to submit false claims to Customs and Border Patrol ("CBP") in order to receive duty drawbacks under 19 U.S.C. § 1313. Specifically, that "[b]etween November 25, 2014 and August, 17, 2017, Pacific Rim caused to be filed at least 68 claims seeking drawbacks totaling at least $7,2016,925 and received at least $6,427,902." Per the indictment, "[t]he drawback claims falsely claimed eligibility for refunds of the customs duties based on the export of commercially interchangeable merchandise under the provisions of 19 U.S.C. §§ 1313(p), when in fact no such export of commercially interchangeable merchandise has occurred."

B. The June 12, 2019 Search Warrant

On June 12, 2019, Special Agent Justin Fletcher of the Internal Revenue Service applied for a search warrant for information associated with the email accounts David.burbidge@trandspacificpolymers.com, JJS@transpacificpolymers.com, JStanka@transpacificpolymers.com, and Josh.clark@transpcificpolymers.com. The affidavit set forth the target offenses as Conspiracy to Defraud the United States by False Claims (18 U.S.C. § 286), Mail Fraud (18 U.S.C. §1341), Wire Fraud (18 U.S.C. § 1343), Conspiracy to Launder Money (18 U.S.C. § 1956 (h)), and Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity (18 U.S.C. § 1957), and sought to collect all evidence, instrumentalities, contraband and/or fruits of these crimes.

The affidavit set forth the timeline of the investigation and the purported facts supporting probable cause. First, it described a previous warrant issued on May 16, 2019, signed by United

States Magistrate Judge, Honorable Sallie Kim, for multiple email accounts hosted by Microsoft. The affiant stated that, pursuant to the Microsoft warrant, he reviewed emails sent to and from Margaret Palacios, an employee of Pacific Rim Traders, and Sarah Stroth, an employee of N.F. Stroth. Then, the affiant relied on those reviewed emails to establish probable cause for the instant warrant. The affiant's facts supporting probable cause were divided into four sections: "TPP Export Americas, LLC Involvement," "TPP's Role Regarding Containers Inspected in South Korea," Additional Bills of Ladings," and "Other Emails." In total, the affiant pointed to fourteen relevant emails giving rise to probable cause. Of those eighteen emails, Mr. Clark was only copied (or "cc'ed") on three.

The warrant sought to authorize employees of Google, LLC to assist in execution of the warrant, and set out a procedure wherein employees of Google, LLC were to isolate the relevant materials described in the warrant and then turn them over to law enforcement to be copied. The warrant sought all of the contents of Mr. Clark's google email account, Josh.clark@transpacificpolymers.com, including:

> (1) the contents of all emails and chat sessions stored in the account from January 1, 2014 to December 31, 2017 including copies of emails and chat chats sent to a from the account, draft emails/chats, the source and destination addresses associated with each email/chat, the date and time at which each email/chat was sent, and the size and length of each email/chat; (2) all records or other information regarding the identification of the account, including full name, physical address, telephone numbers or other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including ay credit or bank account number); (3) all subscriber records for the account; (4) all records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, documents, and files; (5) all records associated with the uploading, sending, and receipt of images, documents, and files, including all time and date stamps, device information, and IP addresses for each interaction; (6) all records pertaining to communications between Google, LLC and any person

> regarding the account, including contacts with support services and records of actions taken; and (7) all records or other information regarding the user's account settings"[1]

Further, after the relevant information was turned over by Google, LLC, law enforcement was to copy all "communications between co-conspirators and others that discuss or otherwise show, in coded or un-coded language:

> (1) information necessary to prepare drawback claims, documentation and support material of imports or exports, invoices, bills of lading, other shipping related documents; (2) knowledge of drawback regulations; (3) modification or knowledge of modification of bills of ladings, invoices, contents of containers, shipping documents, duty drawback claim documents, and exported materials; (4) the preparation of company books and records, the preparation of personal income tax returns, business income tax returns, refund amounts, methods of payment, bank account information, status of prepared and/or filed income tax returns, and knowledge of income tax law and regulations; (5) information regarding law enforcement efforts to investigate or obtain information regarding any of the violations discussed above, influence and/or intimidate potential witnesses, and/or efforts to conceal or hide evidence relating to violations discussed above; (6) information regarding the acquisition of funds received from the drawback claims including bank account information, commission payments, bank account set up instructions, individuals listed with access to bank accounts, method of deposits, acceptance from federal authorities, and information regarding individuals with ability and access to virtually deposit checks; (7) information regarding agreements and business contracts between co-conspirators and others, including monetary agreements and non-monetary agreements; (8) personal identifying information, names, routing numbers, bank account numbers, addresses, dollar amounts, MoneyGram, Western Union, MoneyPak, wiring instructions, pre-paid debit cards, or any other details related to financial accounts or financial transaction, (9) records that show who created, used, or communicated with the account, including records about their identities and whereabouts, insofar as this information constitutes evidence of [the listed offenses]; (10) identification of other accounts, domains, IP addresses, and computers owned or controlled by the same individual(s) controlling each account listed . . .; and (11) the following documents that tend to establish the identity of the person or persons in control of the account: identification documents (such as driver's licenses or passports), photographs, bills, receipts, vehicle registration documents, statements,

[1] Exhibit 2, Attachment B, Section II.

> leasing agreements, personal address books, calendars, daily planners, and personal organizers."[2]

This broad search was based on Mr. Clark only being copied on three emails over a period of three years. Nevertheless, the warrant was issued by Honorable Laurel Beeler on June 12, 2019.

C. The October 25, 2019 Search Warrant

The next warrant was issued four months later, on October 25, 2019, for the Google email accounts mchoy@scm.com, josh.clark@hammetexas.com, js@trfpi.com, jh@trfpi.com, cv@trfpi.com, and jstanka@gmail.com. In the supporting affidavit, Special Agent Benjamin Kurko listed the same target offenses as the previous warrant on June 12, 2019. As to Mr. Clark, this warrant sought information from a different google account – josh.clark@hammertexas.com.

Here, the affiant relied on emails reviewed via previous search warrants, along with a brief statement from another relevant actor, Choy, to support probable cause for the present warrant. The affiant specified fifteen emails which purportedly created probable cause to issue this warrant. Of those fifteen, Mr. Clark was only a party to **two**. The affiant claimed that these facts supported "probable cause to believe that Choy, Stanka, Clark, Sarah Stroth, Neill Stroth, and others working for NF Stroth, Liang of ML Trading, and Beham and others at Pacific Rim Traders participated in a scheme to defraud the United States."[3] The affidavit did not provide examples of crimes being committed by, through, or on behalf of Hammer Trading, LLC ("Hammer Texas").

The October 25, 2019 affidavit set out the same procedure for Google, LLC employees and law enforcement personnel as the June 12, 2019 warrant, with the same scope of items to be seized.

---

[2] Exhibit 2, Attachment B, Section III.
[3] Exhibit 4, para. 39.

Again, despite the scarcity of evidence pertaining to Mr. Clark and his business, Hammer Texas, the warrant was issued by the Honorable Bernard Zimmerman on October 25, 2019.

III. ARGUMENT

A. Mr. Clark Has Standing to Challenge The Warrants

Defendant Clark has standing to challenge the contents of the communications obtained via the June 12, 2019 and October 25, 2019 search warrants because he had a reasonable expectation of privacy in his email accounts Josh.clark@transpacificpolymers.com and Josh.clark@hammertexas.com. Katz v. United States, 389 U.S. 347, 351 (1967). In order for the court to determine whether the seizure was a violation of the Fourth Amendment, the Court must first determine whether Clark "had an actual, subjective expectation of privacy, and second, whether that expectation was a legitimate, objectively reasonable expectation. Id; United States v. Smith, 263 F.3d 571, 582 (2001); Smith v. Maryland, 442 U.S. 735, 740 (1979). In analyzing the subjectivity prong, the Ninth circuit has previously looked to whether the individual treated the property as if it were exclusive to him, finding, for example, in Ziegler 474 F.3d 1138, 1189 (2007), "use of a password on a computer and the lock on a private office door are sufficient evidence of such expectation. United States v. Ziegler, 474 F. 3d 1184, 1189 (2007).

But the expectation must also be objectively reasonable, determined on a case-by case basis. O'Connor v. Ortega, 480 U.S. 709, 718 (1987) ("we have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable"). For example, in Mancusi v. DeForte, 392 U.S. 364 (1968), the Supreme Court found that a union employee had an objectively reasonable expectation of privacy, and therefore Fourth Amendment standing, in the records stored in his office that he shared with several other union employees. The court reasoned,

"[in] such a 'private' office, DeForte would have been entitled to expect that he would not be disturbed except by personal or business invitees, and that records would not be taken except with his permission or that of his union superiors." Id. At 369. The fact that DeForte shared his office with other union employees did not "fundamentally change" the situation.

In contrast, an employer's notice to an employee that email accounts may be monitored undermines the objective reasonableness of the employee's expectation of privacy in an account. See United States v. Angevine, 281 F.3d 1130 (10th Cir. 2002) (professor had no standing to suppress evidence of child pornography located on his office computer which was part of university system network); United States v. Simons, 206 F. 3d 392 (4th Cir. 2000) (official internet usage policy eliminated any reasonable expectation of privacy that employee might otherwise have in copied files); Muick v. Glenayre Electronics, 280 F. 3d 741 (7th Cir. 2002) (employee had no reasonable expectation of privacy in laptop files where employee announced it could inspect laptops it furnished to employees at any time).

1. June 12, 2019 Search Warrant For Google Email Account Josh.Clark@Transpacificpolymers.com

Mr. Clark had a reasonable, subjective expectation of privacy in the email account josh.clark@transpacificpolymers.com. Katz v. United States, 389 U.S. 347 (1967). Mr. Clark's email address belonged solely to him and was password protected – much like a lock on an office door. United States v. Ziegler, 474 F.3d 1184. Moreover, Mr. Clark had a legitimate, objective expectation of privacy in the account. Although his email address included the company name, the company itself, Trans Pacific Polymers, had no oversight over his email account. In fact, Trans Pacific Polymers was a small Limited Liability Company of which Mr. Clark himself owned 37.5%, with the rest being owned by Stanka and Burbidge. There was no managerial hierarchy to suggest that another

employee could oversee or intrude upon Clark's company email account. Rather, the three men acted as separate individuals operating equally under the umbrella of the company, with their own unique conversations, domains, and activities, entirely unencumbered by oversight. Mr. Clark accessed his email account from personal computers as well as his personal cell phone, as evidenced in the signatures of many emails intercepted by the search warrant. If the objective reasonableness of the expectation of privacy is "based upon societal expectations," modern society would deem this email account exclusive and private to Mr. Clark, as our personal devices, and the information we store on them, are considered highly private. See Ziegler. Since Mr. Clark had both a subjective and objective reasonable expectation of privacy in his Trans Pacific Polymers email address, he has sufficient standing to challenge the search warrant issued for the aforementioned account on June 12, 2019.

2. October 25, 2019 Search Warrant For Email Account Josh.Clark@HammerTexas.com

Similarly, Mr. Clark has standing to challenge the search warrant executed on his Josh.clark@hammertexas.com email account because he had a subjective expectation of privacy in that account, as well as an objectively reasonable one. Katz. Mr. Clark had a subjective expectation of privacy over this email account because he was the sole custodian of the account, it was password protected, and he had no reason to suspect anyone else could or would access the account. Objectively, Mr. Clark had a reasonable expectation of privacy because, unlike in Muick, where the company warned employees that they had the right to access employees' email accounts, Mr. Clark was not subject to anyone else's oversight. Mr. Clark operated Hammer Texas, LLC independently, and nothing in the warrant affidavit suggested that Mr. Stanka, Behm, or any other co-defendants similarly operated Hammer Texas or were able to intrude upon his email account. Throughout the entire warrant, Mr. Clark was the only name associated with the Hammer Texas email address.

Because he had a reasonable expectation of privacy in both email accounts, Mr. Clark has standing to challenge the search warrants executed on his google email accounts.

B. The Search Warrants Were Not Supported by Probable Cause and All Evidence Obtained Thereby Should Be Suppressed.

1. Fourth Amendment Requirements

The Fourth Amendment provides: ". . . no Warrants shall issue, *but upon probable cause*, supported by Oath or affirmation, *and particularly describing the place to be searched, and the persons or things to be seized.*" U.S. Const. amend. IV (emphasis added); see also United States v. Galpin, 720 F. 3d 436, 446 (2d Cir. 2013). The purpose of the Fourth Amendment warrant clause is to ensure that "those searches deemed necessary should be as limited as possible." Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

"[T]he specific evil" in this case "is the 'general warrant' abhorred by the colonists, and the problem is not the intrusion *per se*, but of a general, exploratory rummaging in a person's belongings." Id. See also United States v. Rettig, 589 F. 2d 418, 423 (9th Cir. 1978) ("Where evidence is uncovered during a search pursuant to a warrant, the threshold question must be whether the search was confined to the warrant's terms . . . [T]he search must be one directed in good faith toward the objects specified in the warrant . . . It must not be a general exploratory search"). The Constitution limits law enforcement's rights to search only "the specific areas and things for which there is probable cause to search," which requires that "the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." Maryland v. Garrison, 480 U.S. 79, 84 (1987).

The Government's search warrants to search the Mr. Clark's email accounts relied on stale information, were overbroad, and lacked the requisite nexus between the stated facts and the alleged

violations of federal law. Accordingly, the warrants violated the Fourth Amendment, and the evidence seized pursuant to both warrants should be suppressed.

2. The Information Underlying the Warrants Was Stale

"Information underlying a warrant is not stale if there is a sufficient basis to believe, based on a continuing pattern or other good reasons, that the items to be seized are still on the premises." United States v. Schesso, 730 F.3d 1040, 1047 (9th Cir. 2013). Courts must "evaluate staleness in light of the particular facts of the case and the nature of the criminal activity and property sought." United States v. Lacy, 119 F.3d 742, 745 (9th Cir. 1997). In United States v. Greathouse, the Ninth Circuit granted a motion to suppress based on staleness where thirteen months had passed between the time the warrant was executed and the alleged criminal act took place. 297 F. Supp. 2d 1264 (2003). The Court stated, "[i]n the absence of ongoing, continuous criminal activity, this case presents the court with a difficult line-drawing decision." Id. at 1272. The Court relied on United States v. Zimmerman, 277 F.3d 426, 433-34 (3d Cir. 2002), which held that "viewing of a pornographic video file on the defendant's computer six months prior to the execution of the search warrant was too stale, absent any evidence . . . of continuous criminal activity." Greathouse at 1272-3 (citing Zimmerman). In contrast, in United States v. Cramer, the defendant alleged that a warrant was stale because the affidavit relied on two instances from 2007. United States v. Cramer, 2019 U.S. Dist. LEXIS 34959 (D. Or. 2019). The court found it was not stale because, on top of those two instances, the affiant detailed more recent "other aspects of the investigation" including one instance in 2013 and three instances in 2014 which created sufficient basis for probable cause. Id. at 20.

In this instant case, both warrants were stale. The government applied for the first warrant to search josh.clark@transpacificpolymers.com on June 12, 2019. The affiant relied on email communications to support probable cause, many of which dated back to 2014. The most recent

emails were from 2017, two years before the instant application was filed. The only emails implicating Mr. Clark in any way were three emails to which he was **copied** in 2016 – three years before the affiant decided to apply for the search warrant in this case. In fact, the relevant company, Trans Pacific Polymers, dissolved in 2017 and Mr. Clark created an entirely new and separate business for himself, Hammer Trading, LLC, in the time since then. The second warrant for josh.clark@hammertexas.com was overbroad for the same reason. The affidavit only referenced two relevant emails from 2017, over two years prior, to establish probable cause. There was no sufficient basis to believe that, "based on a continuing pattern or other good reasons" the sought-after information was still present in either email account. U.S. v. Greathouse, 297 F. Supp. 2d 1264 (2003).

3. The Warrants Were Unconstitutionally Overbroad

The Fourth Amendment requires that search warrants describe items to be seized and the premises or persons to be searched with sufficient particularity. The particularity requirement bars overbroad search warrants. In re Google Email Accounts Identified in Attachment A, 92 F. Supp. 3d 944, 950 (2015). The Ninth Circuit has previously held, "overbreadth is a tailoring question: does the proposed warrant limit the government's search to the specific places that must be inspected to confirm or dispel the suspicion that gave rise to probable cause?" Id. With the proliferation of digital data and electronically stored information, this court has previously warned against the dangers of overbroad search warrants:

> "we recognize the reality that over-seizing is an inherent part of the electronic search process and . . . when it comes to the seizure of electronic records, this will be far more common than in the days of paper records. This calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the

> government to gain access to data which it has no probable cause to collect." United States v. Comprehensive Drug Testing, Inc., 621 F. 3d 1162, 1177 (2010).

The requirements of such judicial vigilance have been illuminated by this court multiple times. In In Re Google Email Accounts, the court relied on Hill to demonstrate the particularity requirement, quoting "there must be some threshold showing before the government may 'seize the haystack to look for the needle.'" In re Google at 954 (quoting United States v. Hill, 459F.3d 966, 975 (2006)).

In re Google involved "a probable-cause showing by the government that implicates only a few email transactions, yet the government seeks to obtain the Gmail email accounts in their entirety." Id. at 952. The search warrant affidavit stated that six Gmail accounts responded to a Craigslist advertisement soliciting sex with underage girls. Based on those facts alone, the court held there was probable cause to believe that the "email responses to the advertisement contain[ed] evidence of a crime." Id. at 952. Regardless, the search warrant was overbroad because "it would authorize the government to seize and search the *entirety* of the six Gmail accounts, even though the government . . . only established probable cause to look at a small number of emails within a narrow date range." Id. (emphasis in original).

In contrast, in United States v. Hay, 231 F.3d 630 (2000), the government's affidavit stating that the defendant, Hay, likely had 19 images of child pornography on his computer, but the affiant was unable to specify exactly where the images were located on the computer. Hay at 637. The affidavit in Hay contained a good deal of evidence showing that the 19 files were sent to Hay not via email but were downloaded to his computer system via FTP, "a protocol for the direct transfer of files." Id. at 634. Pursuant to the search warrant, law enforcement searched and seized Hay's computer, software, computer disks, and seven Zip drives. Id. at 633. The court upheld the warrant, relying on its holding

in Lacy, quoting "in this case no more specific description of the computer equipment sought was possible." Id. at 637 (quoting United States v. Lacy, 119 F. 3d 742, 746 (1997)).

a. June 12, 2019 Warrant was Overbroad

The June 12, 2019 search warrant was similar to the warrant in In re Google Accounts because it "expand[ed] the scope of the government's search beyond the places implicated by the probable cause showing." In re at 953. Firstly, the affidavit only provided three limited instances in which Mr. Clark was included in any discussions about duty drawback, claims, or bills of lading.

The first section of the affidavit, "TPP's Role Regarding Containers Inspected in South Korea," lists five pertinent emails.[4] Of those five emails, Mr. Clark was only **copied** on one – an email on April 16, 2017 wherein David Burbidge sent to Margaret Palacios "attachments containing invoices and bills of lading listed below."[5] There are no facts in the affidavit to establish that those invoices or bills of ladings were, at the time Mr. Clark was party to that email, fraudulent or modified.

In the second section, "Additional Bills of Ladings," the affiant relied on his review of some number of bills of lading sent from TPP to PRT and then to N.F. Stroth. Again, Mr. Clark took no active role in any of these emails, was only copied. The affiant failed to specify how many bills of ladings he reviewed, or the dates of the emails he reviewed. Instead, he stated generally:

> "I reviewed several bills of ladings received from CMA CGM that contained different information than the bills of ladings provided by TPP to PRT. The bills of ladings were sent from Burbidge (David.burbidge@transpacificpolymers.com) and **copied** to Clark (josh.clark@transpacificpolymers.com) or sent from Stanka (jjs@transpacificpolymers.com)."[6]

---

[4] Specifically, one email on October 31, 2014, two emails on April 1, 2016, one email on March 3, 2017, and one on March 10, 2017.
[5] Ex. 2, Para. 34
[6] Ex. 2, Para 46.

The affiant then "summarized" three bills of ladings he found relevant out of the "several bills of ladings" he reviewed. Mr. Clark was not the sender or recipient of any of the aforementioned bills, but was copied on two emails. The affiant did not specify who those emails or bills were sent to. In the third section, "Other E-Mails," Mr. Clark is not implicated at all. In total, Mr. Clark is only **copied** on three emails in the entire warrant. Such scant underlying facts fail to support probable cause, and certainly do not necessitate an in-depth search of his entire google email account.

Much like the warrant in In re Google Accounts, the government sought to obtain the entire email account belonging to Josh Clark, far beyond what the underlying facts supported. Unlike in Hay or Lacy, where "a more precise description [was] not possible," the affiant here could have more narrowly tailored the warrant to only search for evidence of the crimes alleged. The affiant named the specific transactions that raised a red flag, and could have limited the search for evidence to those specific transactions, dates, claim numbers or bills of ladings. Instead, he sought the seizure of Mr. Clark's entire google account, including photos, IP information, identity information, and more.

b. October 25, 2019 Warrant was Overbroad

The October 25, 2019 warrant was also overbroad because it sought to seize information from Mr. Clark's email account for a business that was completely unrelated to the alleged fraudulent scheme. As previously stated, the affiant rested his probable cause on the contents of emails intercepted from a previous warrant. While those emails mentioned multiple people, companies, shipments, and other information relevant to the alleged crimes (or at least the subject of those crimes – imports and exports), Hammer Trading, LLC was not once mentioned in any of those emails. Mr. Clark was only a sender or recipient to two emails - out of fourteen mentioned in the affidavit. Similar to the previous warrant affidavit, here the affiant specified the attachments to those emails, including pdf documents. The affiant could have limited the search to only information relative to the

contents of those specific attachments, but instead sought to search the entirety of Mr. Clark's google account.

4. The Warrants Do Not State a Sufficient Nexus Between the Underlying Factual Information and the Alleged Crimes

For a search warrant to be valid, it "must be supported by an affidavit establishing probable cause." United States v. Stanert, 762 F.2d 775, 778 (9th Cir. 1985). Such probable cause exists when, under the totality of the circumstances, "there is a fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983). When reviewing a magistrate judge's determination that probable cause existed for a warrant, the district court is "limited to the information and circumstances contained within the four corners of the underlying affidavit." Stanert, 762 F.2d at 778. The supporting affidavit "must establish a reasonable nexus between the crime or evidence and the location to be searched." United States v. Crews, 502 F.3d 1130, 1136-37 (9th Cir. 2007) (citing United States v. Chavez-Miranda, 306 F.3d 973, 978 (9th Cir, 2002)). Any conclusions offered by the affiant that are unsupported by underlying facts are not sufficient to establish probable cause. United States v. Underwood, 725 F.3d 1076, 1081 (9th Cir, 2013). The issuance of a warrant is only upheld "if the issuing judge 'had a substantial bases' for concluding [that] probable cause existed based on the totality of the circumstances." Ewing v. City of Stockton, 588 F.3d 1218, 1223 (9th Cir. 2009).

In United States v. Pippin, the affidavit failed to show that a crime had been committed as to the specific email addresses listed in the warrant. United States v. Pippin, 2017 U.S. Dist. LEXIS 66841 at 11. The only fact the affiant used to support probable cause was that the National Center for Missing and Exploited Children listed the email address as a secondary account for the defendant. Although a search of the defendant's primary email account was supported by probable cause, the

court held, "[w]ithout an additional reason to suggest evidence would be found in the secondary email, there was not probable cause." Id.

a. June 12, 2019 Warrant

Firstly, as stated above, the affiant's facts underlying probable cause rested solely on Mr. Clark's attachment to **three** emails – out of fourteen – in which he was merely **copied** (or "cc'ed").

Secondly, the emails intercepted between other actors in the affidavit **negate** probable cause for Mr. Clark. For example, "On March 26, 2014, Behm emailed Jaques Robichard, Palacios, and Eric Chen from PRT and copied Stanka: 'No one is to talk to anyone about DDB, customs, Jetway, anyone . . . All communication thru Josh [Stanka] only and myself!'"[7] This email suggests that the few people included in the email were privy to information about duty drawback ("DDB") that others cannot or should not know. Mr. Clark was not included in the email. This email explicitly reveals the small circle of people who had knowledge of the scheme, to the exclusion of Mr. Clark. Similarly, Stanka emailed Dale Behm saying "Hey my friend Working on this new claim for you" and discussed how, when and where to send a wire, which suggests that Stanka was in charge of financial decisions for TPP.[8] If Mr. Clark were a part of the alleged fraudulent scheme, he would not be excluded from pertinent emails about the subject matter.

The affiant used these email conversation to establish probable cause to search email accounts belonging to Joshua Stanka and David Burbidge, since the affiant reviewed multiple emails in which Burbidge and Stanka were involved. Particularly, Stanka was party to numerous email conversations that discussed shipments, communications with the brokerage firm N.F. Stroth, drawback claims, and other information relevant to the alleged crimes. But Mr. Clark's level of involvement simply did

[7] Ex. 2, Para. 55
[8] Ex. 2, Para. 55

not rise to the same level as the other actors. The three emails simply do not create a reasonable nexus between the crimes alleged and Mr. Clark's email account.

Because of the attenuated nexus between Mr. Clark's email account and the alleged fraudulent scheme, as well conversations between other actors explicitly excluding Mr. Clark from insider information, the search warrant is not supported by probable cause and thus, all fruits of it must be suppressed.

b. October 25, 2019 Warrant

In the affidavit relevant to the present case, the affiant did not provide facts linking Mr. Clark's Hammer account to the alleged scheme. Paragraph 8 reads: "I believe that TPP was dissolved in approximately August 2017 and that Hammer took over some of its operations . . . [and] continues to presently operate in the same manner that TPP did, with fundamentally some of the same principals, physical office location, and clients (both importers and exporters)." The affiant claims that "[Michael] Choy received, via email, original bills of lading from Liang and modified them before sending them, via email, in modified format to Stanka and Clark."[9]

Thereafter, the affiant cites to 15 different email exchanges that purportedly support probable cause to believe that Mr. Clark, through his Hammer Texas email account, was engaged in a criminal conspiracy to defraud the United States. Only **two** of those fifteen email exchanges include Mr. Clark. On August 24, 2017, Mr. Clark emailed Choy with the subject line "This Weeks SI," which the affiant believes stands for "shipping instructions." On August 29, 2017, Choy emailed Mr. Clark and Stanka with the subject line "BLs 8/25," which the affiant believes stands for "bills of lading."

[9] If Michael Choy was modifying the bills of lading and then sending it to Stanka and Clark, the government would have to prove that Clark knew Choy was modifying them, or otherwise was "in on the scheme." The affidavit did not lay out facts that support the contention that Clark was in on it.

The affiant also relies on an interview he conducted with Choy, in which Mr. Choy said he continues to do business with Clark since the dissolution of TPP in mid-2017.

None of these facts create the requisite probable cause to believe that Mr. Clark was engaged in any criminal activity. There are no facts to suggest that Stanka or Burbidge were involved with the management of Hammer Trading. In fact, by the time Mr. Clark opened his new email account at Hammer Texas dot com, TPP had already dissolved. Mr. Clark created his own business, Hammer Trading LLC, where he continued working in imports and exports – a wholly legitimate and legal business – completely unrelated to TPP. The fact that he was party to two emails in August 2017 which discussed the subject matter of his livelihood – shipping instructions and bills of lading - does not point to nefarious conduct on his part.

The government cannot transfer whatever probable cause they purport to have for TPP to Hammer, an entirely different entity. The search of Mr. Clark's Hammer Texas email account constitutes an egregious overstep on the government's behalf, completely lacking in probable cause, and all fruits of that search must be suppressed.

C. The Good Faith Exception Does Not Apply

Because both warrants were insufficient to establish probable cause, the good faith doctrine does not apply here. Under the good faith doctrine, law enforcement agents may rely on a search warrant so long as the affidavit supporting the warrant is "sufficient to 'create disagreement among thoughtful and competent judges as to the existence of probable cause.'" United States v. Hove, 848 F.2d 137, 139 (9th Cir, 1988) (quoting United States v. Leon, 468 U.S. 897, 926 (1984). However, the good faith exception does not apply to a warrant and affidavit that plainly fails to show probable cause. See United States v. Underwood, 725 F.3d 1076, 1086 (9th Cir. 2013). In United States v. Pippin, the court declined to apply the good faith exception because "the affidavit included many facts that at

first glance suggested probable cause, but when combed through, a significant disconnect reveals itself, and the affidavit ultimately proves insufficient."

In this case, for reasons stated above, both warrants plainly failed to establish probable cause.

IV. CONCLUSION

The affidavits supporting the warrants issued on June 12, 2019 and October 25, 2019, for email accounts josh.clark@transpacificpolymers.com and josh.clark@hammertexas.com, respectively, lacked probable cause. The affidavits relied on stale information, were overbroad, and lacked any reasonable nexus between the facts and alleged crimes committed. Thus, the warrants issued were violative of the Fourth Amendment of the United States Constitution and all fruits of those warrants should be suppressed.

Respectfully submitted,

Dated: October 14, 2021

s/Drew Findling

Drew Findling
PHV-21739-2019
Findling Law Firm P.C.
3490 Piedmont Road, Suite 600
Atlanta, GA 30305
404-460-450